UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,309	02/19/2004	Ari Juels	4414-35	7635

80167 7590 08/04/2008

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
HOLLOWAY III, EDWIN C	
ART UNIT	PAPER NUMBER
2612	

MAIL DATE	DELIVERY MODE
08/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,309	JUELS, ARI	
	Examiner	Art Unit	
	Edwin C. Holloway, III	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 9-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *17-19,21 and 22* is/are allowed.

6)☒ Claim(s) *1-7,9-16,20,23-28 and 30-33* is/are rejected.

7)☒ Claim(s) *29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

EXAMINER'S RESPONSE

1. A request for continued examination under 37 CFR 1.114 was filed in this application after appeal to the Board of Patent Appeals and Interferences, but prior to a decision on the appeal. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 5-20-2008 has been entered. Claims 1-7 add 9-33 are pending. The examiner has considered the presentation of claims in view of the disclosure and the present state of the prior art. And it is the examiner's position that claims 1-7, 9-16, 20, 23-28, and 30-33 are unpatentable for the reasons set forth in this Office action:

Applicant is notified that the examiner listed on the prior Office action is no longer examining this case. See the contact information at the end of this Office action for identification of the current examiner.

Specification

2. The disclosure is objected to because of the following informalities: The reference to related application data should be updated to indicate 10/673,540 was allowed as US Patent No.

6970070.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-2, 4-7, 20, 23-25, 30, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hughes (US 6842106) in combination with Dannhaeuser (US 4928098) and Rodgers (US 6340932).

Regarding claims 1 and 2, Hughes discloses a method for use in an RFID system comprising tags (RFID devices 44) and reader (32) which communicates with the tags {abstract, fig. 2}, the method comprising the steps of:

associating a plurality of pseudonyms (multiple secret key value 66 or 68) with the tag (RFID device 44) {col. 5, lines 47-50; col. 6, lines 32-33, lines 64-65; col. 7, lines 51-53}; and transmitting from the tag (RFID device 44) pseudonyms in response to different reader queries of the RFID device {col. 6, lines 15-18, lines 27-28}. In this case, the pseudonyms are converted to pseudo random number based on the key value {col. 6, lines 18-26};

wherein an authenticator (authorized verifier) is able to determine that the different transmitted pseudonyms (multiple

key value) are associated with the same tag {col. 5, lines 61-64; col. 6, lines 42-46}. In this case, the reader doubles as an authenticator {col. 6, lines 16-18}.

Although Hughes discloses multiple key values {col. 6, lines 64-65; col. 7, lines 52-58}, Hughes does not expressly disclose "transmitting the different ones of the pseudonyms (multiple secret key values)". Also, Hughes discloses the multiple keys correspond to levels (col. 7 lines 52-53, but does not expressly disclose "wherein one or more of the pseudonyms each comprise a portion of an identifier of the RFID device."

Dannhaeuser discloses storing plurality of pseudonyms in algorithmic or tabular form {Dannhaeuser, col. 3, lines 42-48} in both a transmitter and receiver (also shown in the table of column 3) wherein the plurality of pseudonyms are cyclically traversed by the transmitter and receiver during transmission {Dannhaeuser, col. 3, lines 1+}. Dannhaeuser discloses that this feature foils attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses {Dannhaeuser, col. 1, lines 26+}. The systems of Dannhaeuser and Hughes are analogous art because they are from the same field of endeavor (wireless communications), and the same problem solving area. Hughes is concerned with communication security {Hughes, col. 2, lines 29+}. Obviously,

the teaching of Dannhaeuser is desirable in the system of Hughes because it increases the communication security of Hughes. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the method of Hughes to "transmit the different ones of the multiple secret key values (pseudonyms)", as taught by Dannhaeuser, because this feature increases security to a wireless communication by foiling attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses.

Rodgers discloses an analogous art RFID method, apparatus (device) and system wherein the device includes a relatively long identification number broken up into several access codes, each associated with a different level in a sequence. See protocol 5 in table 2 in col. 19 and col. 21 lines 40-61. The RFID device (transceiver 201) responds to an interrogation command of a particular level by transmitting a reply with the partial (sub) identification number corresponding to that level (col. 25 lines 17-52).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have included in the combination applied above the a relatively long identification number broken up into several access codes as disclosed in Rodgers so that one or more of the pseudonyms each comprise a

portion of an identifier of the RFID device because this is an obvious alternative to multiple separate codes of a sequence and would provide advantages such as quick response.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the inventions of Hughes, Dannhaeuser and Rodgers to provide the limitations of claims 1 and 2.

In claim 4, the tag is configured to authenticate itself to an authenticator only after the authenticator has authenticated itself to the tag {Hughes, col. 7, lines 32-47}.

In claim 5, the authenticator authenticates itself to the tag by releasing to the tag a first challenge value (authentication value) unique to a given pseudonym transmitted by the tag {Hughes, col. 7, lines 16-23}.

In claim 6, the tag authenticates itself to the authenticator by releasing to the authenticator a second challenge value (authentication value) unique to a given pseudonym transmitted by the RFID device {Hughes, col. 7, lines 24-31}.

In claim 7, one or more of the pseudonyms each comprise an identifier of the tag {Hughes, col. 6, lines 57-65}. In this case, the tag key value identifies the tag.

In claim 20, a verifier is configured to store for a given

RFID device Tx an address no. (a static identifier idx) corresponding to at least one pseudonym of Tx {Dannhaeuser, Fig. 2, col. 3 lines 1-48}.

In claim 23, a verifier specifies value identifying a particular pseudonym {Dannhaeuser, col. 3, lines 49+}.

In claim 24, the RFID device determines which of the plurality of pseudonyms to transmit responsive to a given reader query based at least in part on timing information {Dannhaeuser, paragraph bridging cols. 3 and 4}.

In claim 25, the method of claim 1 wherein the RFID device incorporates a pseudorandom number generator, where fx(i) represents an output of the pseudorandom number generator for index i, where x is a key value (seed) associated with the RFID device {Hughes, col. 5, lines 53-64}.

Claims 30 and 32 recite a system/apparatus for practicing the method of claim 1 and therefore are rejected for the same reasons applied above to claim 1.

Claim 33 recites the limitations of claim 1 that would have been obvious for the same reasons applied above. Further, claim 33 recites the limitation of the pseudonyms are determined by utilizing an updateable set of one-time pads (index designators) maintained in the device as shown in steps S1- S6 of the flowchart in figure 3 of Hughes {Hughes, col. 6, lines 12-46}.

Also see Dannhaeuser, col. 4, lines 5-24.

5. Claims 3 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hughes (US 6842106) in combination with Dannhaeuser (US 4928098) and Rodgers (US 6340932) as applied above and further in view of Turner (US 6724895).

In claim 3, Hughes does not disclose expressly "the transmitted pseudonyms are authenticated by an authenticator (verifier) other than the reader".

Turner, in the same field of endeavor, discloses having a plurality of readers/verifiers in an RFID system {col. 4, lines 40-42}. Since a verifier is also a reader {Turner, Figure 1}, clearly, anyone of them is the reader and anyone of them is the verifier. And since the reader of Hughes is also an authenticator {Hughes, col. 6, lines, 15-16}, a plurality of readers in the system of Hughes, as evidenced by Turner, would have an authenticator authenticating the transmitted pseudonym that is other than the reader. Therefore, at the time of the invention, it would have been obvious to one of ordinary skill in the art to have a plurality of readers in the combination applied above, as evidenced by Turner, wherein an authenticator authenticates the transmitted pseudonym that is other than the reader. Also, Turner states that the verifier 16 may form part

of the reader or may be a separate unit (col. 4 lines 66-67). As disclosed in Turner, verifier other than (separate from) the reader would have been an obvious alternative to verifier in the reader.

Claim 31 recites a system with a plurality of RFID devices and readers for practicing the combination of method claims 1 and 3, and is therefore rejected for the same reasons applied above.

6. Claims 9-13, 14-16 and 26, are rejected under 35 U.S.C. 103(a) as being unpatentable over Hughes (US 6842106) in combination with Dannhaeuser (US 4928098) and Rodgers (US 6340932) as applied above and further in view of Furuta (US 6225889).

In claims 9-13, the combination applied above includes pseudonyms (multiple secret key values) stored in the RFID device as an ordered list of pseudonyms {Hughes, col. 7, lines 52-53; Dannhaeuser, Fig. 3}, but Hughes does not expressly disclose "the step of designating a particular one of the pseudonyms as a current pseudonym and, in response to a given reader query, transmitting the current pseudonym, wherein over a plurality of reader queries the pseudonym designated as the current pseudonym periodically cycles through the list of

pseudonyms."

Furuta, in the same field of endeavor (transponder systems), discloses a method of producing rolling codes between a vehicle transceiver 2 (analogous to the claimed reader) and key transceiver 1 (analogous to the claimed RFID device). The rolling codes are constantly changed by cycling through a different one of a plurality of initial code variables (pseudonym) stored in the memory (5) of the vehicle transceiver 2, shown in Figure 3 {Furuta, col. 5, lines 13-26}. Initially, one of the plurality of the initial code variable stored in the memory (5) of the vehicle transceiver 2 is designated as the current initial code variable, transmitted to the RFID device and stored in the memory of the RFID device (as claimed in 10 and 12) {Furuta, col. 4, lines 17-29}. So that in response to an as needed initial reader query (as claimed in 11), the current initial code variable stored in the memory of the RFID device is used to produce a unique rolling code {Furuta, col. 6, lines 53+} and transmitted to the reader {Furuta, col. 7, lines 11+}. In the case of a mismatched determination, a given period of time is given to a user to transmit another rolling code (as claimed in 13) {Furuta, col. 8, lines 4- 11}. Obviously, these features are desirable in the combination applied above because it provides a high degree of security without compromising

system cost, to one of ordinary skill in the art.

In claims 14-16, the initial code variable may be altered sequentially (as claimed in 14) by the reader {Furuta, col. 8, lines 60+}, in response to receipt of refresh information (as claimed in 15) {Furuta, col. 8, lines 18-22}, after the current initial code variable is determined to be invalid (as claimed in 16) {Furuta, col. 7, lines 63+}. Furuta discloses that the method above is capable of producing rolling codes with a high degree of security using a simple algorithm that do not require large storage capacity {Furuta, col. 1, lines 61-65}. Hughes is concerned with tradeoffs between level of security and system cost {Hughes, col. 7, lines 1-3}. Obviously, these features are desirable in the combination applied above because they provides a high degree of security without compromising system cost, to one of ordinary skill in the art.

In claim 26, the method of claim 25 wherein the RFID device generates the plurality of pseudonyms as pseudonyms α1 =f(1), α2 =f(2) ..... αk =f(3) {Furuta, col. 8, lines 60-65}.

7. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hughes (US 6842106) in combination with Dannhaeuser (US 4928098) and Cole (US 7187267).

Regarding claim 27 Hughes discloses a method for use in an

RFID system comprising tags (RFID devices 44) and reader (32) which communicates with the tags {abstract, Fig. 2}, the method comprising the steps of:

associating a plurality of pseudonyms (multiple secret key value 66 or 68) with the tag (RFID device 44) {col. 5, lines 47-50; col. 6, lines 32-33, lines 64-65; col. 7, lines 51-53}; and transmitting from the tag (RFID device 44) pseudonyms in response to different reader queries of the RFID device {col. 6, lines 15-18, lines 27-28}. In this case, the pseudonyms are converted to pseudo random number based on the key value {col. 6, lines 18-26};

wherein an authenticator (authorized verifier) is able to determine that the different transmitted pseudonyms (multiple key value) are associated with the same tag {col. 5, lines 61-64; col. 6, lines 42-46}. In this case, the reader doubles as an authenticator {col. 6, lines 16-18};

wherein the RFID device incorporates a pseudorandom number generator, where fx(i) represents an output of the pseudorandom number generator for index i, where x is a key value (seed) associated with the RFID device {Hughes, col. 5, lines 53-64}.

Although Hughes discloses multiple key values {col. 6, lines 64-65; col. 7, lines 52-58}, Hughes does not expressly disclose "transmitting the different ones of the pseudonyms

(multiple secret key values)". Also, Hughes discloses the multiple keys correspond to levels (col. 7 lines 52-53), but does not expressly disclose "wherein the RFID device and a verifier of the system attempt to maintain a common counter dx unique to the RFID device, and share the seed kx"

Dannhaeuser discloses storing plurality of pseudonyms in algorithmic or tabular form {Dannhaeuser, col. 3, lines 42-48} in both a transmitter and receiver (also shown in the table of column 3) wherein the plurality of pseudonyms are cyclically traversed by the transmitter and receiver during transmission {Dannhaeuser, col. 3, lines 1+}. Dannhaeuser discloses that this feature foils attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses {Dannhaeuser, col. 1, lines 26+}. The systems of Dannhaeuser and Hughes are analogous art because they are from the same field of endeavor (wireless communications), and the same problem solving area. Hughes is concerned with communication security {Hughes, col. 2, lines 29+}. Obviously, the teaching of Dannhaeuser is desirable in the system of Hughes because it increases the communication security of Hughes. At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the method of Hughes to "transmit the different ones of the multiple secret key values

(pseudonyms)", as taught by Dannhaeuser, because this feature increases security to a wireless communication by foiling attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses.

Cole discloses an analogous art RFID method, apparatus (tag) and system wherein the tag (and authentication database) include a counter incremented with each authentication to provide a tag response code depending on the count (col. 5 lines 39-57) and col. 7 lines 4-29. The code may be by scrambled (col. 7 lines 39-56) corresponding to encryption of a key as in Hughes to secure the communication against eavesdropping.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have included in the combination applied above the RFID device and a verifier of the system attempt to maintain a common counter dx unique to the RFID device in view of the counter 55 of Cole suggested by the counters in col. 3 lines 49-51 of Dannhaeuser, and to share the seed kx in view of the scrambling of the tag identity in Cole and suggested by the private key {Hughes, col. 5, lines 46-50} that corresponds to applicant's seed and would have been desirable in the combination in order to secure the communication against eavesdropping.

Therefore, it would have been obvious to one of ordinary

skill in the art to combine the inventions of Hughes, Dannhaeuser and Cole to provide the limitations of claim 27.

8. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hughes (US 6842106) in combination with Dannhaeuser (US 4928098) and Cole (US 7187267) as applied above and further in view of Saliga (US 5373034).

Regarding claim 28, the combination applied above does not expressly disclose "wherein in order to determine which RFID device is associated with a given incoming value α, the verifier performs a lookup in a list {fkx (dx)} of current α values for a plurality of RFID devices."

Saliga discloses an analogous art security system and method wherein authorization is provided by stepping through plural tables of code segments wherein the access control equipment includes a separate table of code segment values for each user in col. 4 line 59 - col. 5 line 19 corresponding to a list of current values for a plurality of devices.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have included in the combination applied above the limitations of claim 28 as disclosed by Saliga in order to allow authentication of plural devices for controlling access for a plurality of users.

Allowable Subject Matter

9. Claims 17-19 and 21-22 are allowed.

10. Claim 29 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The cited prior art does not teach nor suggest an RFID device computes pseudonym $\alpha_d = f(bk + d)$ for a given counter value d and the verifier provides a subsequent instruction to increment base value b.

Response to Arguments

11. Applicant's arguments, see the remarks on page 9 of the response filed 5-20-2008, with respect to the rejection(s) of claim(s) 1-7, 9-16, 20, 23-26 and 30-33 under 35 USC 103 have been fully considered and are persuasive. Therefore, the prior rejection has been withdrawn. Also, claims 8 and 28 were objected to as including allowable subject matter by the prior examiner. However, upon further consideration, a new ground(s) of rejection is made in view of Rodgers (US 6340932B1) to a long ID number broken up into several shorter access codes corresponding to the limitation added from canceled claim 8 to amended claims 1-7, 9-16, 20, 23-26 and 30-33. Also, Cole (US007187267B2) is applied to disclose the counters of claim 27 and Saliga (US 5673034) for the tables listing codes for plural

devices of claim 28.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Bauhahn (US 7239229) discloses RFID transmitting part of ID.

CONTACT INFORMATION

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edwin C. Holloway, III whose telephone number is (571) 272-3058. The examiner can normally be reached on M-F from 9:00 to 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian Zimmerman, can be reached on (571) 272-3059.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

8/5/2008 /Edwin C. Holloway, III/
(571) 272-3058 Primary Examiner, Art Unit 2612